
MCSE Guide to Designing Microsoft Windows 2000 Security

Conan Kezema, Stanley Reimer

**COURSE
TECHNOLOGY**
★
THOMSON LEARNING



MCSE Guide to Designing Microsoft Windows 2000 Security

by Stanley Reimer and Conan Kezema

Product Manager:

Charles Blum

Production Editor:

Christine Spillett

Developmental Editor:

Moirag Haddad

Quality Assurance Manager:

John Bosco

Quality Assurance Tester:

Nicole Ashton

Associate Product Manager:

Tim Gleeson

Editorial Assistant:

Nick Lombardi

Marketing Manager:

Toby Shelton

Text Designer:

GEX Publishing Services

Compositor:

GEX Publishing Services

Cover Design:

Joseph Lee, Black Fish Design

COPYRIGHT © 2002 Course Technology,
a division of Thomson Learning, Inc.
Thomson Learning™ is a trademark
used herein under license.

Printed in Canada

1 2 3 4 5 6 7 8 9 WC 06 05 04 03 02

For more information, contact
Course Technology, 25 Thomson Place,
Boston, Massachusetts, 02210.

Or find us on the World Wide Web
at: www.course.com

ALL RIGHTS RESERVED. No part
of this work covered by the copyright
hereon may be reproduced or used in
any form or by any means—graphic,
electronic, or mechanical, including
photocopying, recording, taping, Web
distribution, or information storage and
retrieval systems—without the written
permission of the publisher.

For permission to use material from this
text or product, contact us:
Tel (800) 730-2214
Fax (800) 730-2215
www.thomsonrights.com

Disclaimer

Course Technology reserves the right to
revise this publication and make
changes from time to time in its content
without notice.

ISBN 0-619-01688-4

BRIEF
Contents

PREFACE	xi
CHAPTER ONE Identifying Security Risks	1
CHAPTER TWO Corporate Components to Security Planning	21
CHAPTER THREE Securing Resources on Windows 2000 Servers	57
CHAPTER FOUR Designing Active Directory for Security	109
CHAPTER FIVE Implementing a Public Key Infrastructure	169
CHAPTER SIX Securing Network Services	219
CHAPTER SEVEN Securing Network Communications	265
CHAPTER EIGHT Securing Access for Remote Access Users	295
CHAPTER NINE Securing Access Between Corporate Locations	341
CHAPTER TEN Designing Secure Access to the Internet	377
APPENDIX A Exam Objectives for MCSE Certification	413
GLOSSARY	419
INDEX	427

TABLE OF Contents

PREFACE

xi

CHAPTER ONE

Identifying Security Risks

1

Internal Security Risks

2

Access to Information

3

Access to Network Traffic

4

Access to Administrative Rights

5

Access to Network Services

6

External Security Risks

8

Access to the Internal Network

8

Sending Information on Public Networks

10

Managing Security Risks

11

Chapter Summary

12

Key Terms

13

Review Questions

13

Setup For Hands-on Projects

17

Hands-on Projects

18

Case Projects

19

CHAPTER TWO

Corporate Components to Security Planning

21

Identifying Business Models

22

Ownership and Control

23

Products and Services

26

Business Processes

28

Corporate Geographic Scope

31

Corporate Management Model

32

Relationships with Other Organizations

35

Identifying Corporate Strategies and Goals

36

Corporate Vision and Goals

36

Growth Strategies

37

Integration with IT

38

Identifying IT Administrative Structures

39

Identifying the Current Technical Environment

40

Corporate Locations

41

Networking Infrastructure

42

Networking Services

44

Network Administration

45

Configuration Change Management

46

Client Requirements

46

Identifying the Current Security Model	48
Physical Security	48
Network Security	49
Chapter Summary	50
Review Questions	51
Hands-on Projects	54
Case Projects	56

CHAPTER THREE

Securing Resources on Windows 2000 Servers **57**

Implementing User Authentication	58
Kerberos v5 Authentication	59
NTLM Authentication	62
Down-level Client Authentication	63
Certificate-based Authentication	63
Remote Access Authentication	65
Accessing Resources	65
Security Principals	66
Access Tokens	66
Access Control Lists	67
Securing File Resources	70
Share Permissions	70
NTFS Permissions	74
Combining Share and NTFS Permissions	77
Encrypting File System	78
The File Encryption Process	79
Implementing EFS	79
Managing Data Recovery	80
Securing Printers	81
Setting Printer Security	81
Securing The Registry	82
Default Registry Settings	85
Configuring an Audit Policy	86
Managing Event Logs	89
Planning Best Practices	93
Chapter Summary	95
Key Terms	95
Review Questions	97
Setup for Hands-on Projects	102
Hands-on Projects	102
Case Projects	107

CHAPTER FOUR

Designing Active Directory for Security **109**

Active Directory Components	110
Active Directory Domains	111
Active Directory Trees	111
Active Directory Forests	112
Organizational Units	113
Sites	114
Domain and Forest Design—Security Planning Implications	115
Securing Active Directory	116
Security Templates	117

Managing Account Policies	125
Password Policy	125
Account Lockout Policy	126
Kerberos Policy	127
Account Policies Security Implications	127
Delegating Administrative Tasks	128
Permission Inheritance	129
Managing Delegation	130
Designing Active Directory for Delegation	137
Implementing Security Groups	139
Group Types and Scopes	139
Default and Built-in Groups	140
Managing Security Groups	143
Implementing Group Policies for Security	144
Group Policy Overview	144
Managing Group Policies	147
Planning Best Practices	155
Chapter Summary	155
Key Terms	156
Review Questions	157
Hands-on Projects	161
Case Projects	167

CHAPTER FIVE

Implementing a Public Key Infrastructure	169
Public Key Infrastructure (PKI) Overview	170
Public and Private Keys	170
Certificate Authorities	174
Application Support	177
Planning and Implementing a Public Key Infrastructure	182
Designing the Certificate Server Hierarchy	182
Planning the Certificate Server Type	184
Identifying Client Certificate Needs	186
Windows 2000 Certificate Server Implementation	188
Installing Certificate Servers	188
Configuring Servers to Use Certificates	191
Managing Certification Requests	196
Managing Certification Revocations	197
Mapping User Accounts to Certificates	199
Certificate Server Client Implementation	201
Integration with Third-Party CAs	205
Choosing a Third-Party PKI Solution	206
Integrating Windows 2000 PKI and a Third-Party PKI	207
Planning Best Practices	207
Chapter Summary	208
Key Terms	209
Review Questions	210
Hands-on Projects	214
Case Projects	217

CHAPTER SIX**Securing Network Services 219**

Implementing DNS and DHCP Security	220
DNS Zones in Windows 2000	221
DNS and DHCP Integration Concepts	224
Securing Dynamic Updates to DNS	226
Implementing Remote Installation Services Security	231
RIS Requirements	232
Configuring RIS	232
Installing Windows 2000 Professional Clients Using RIS	233
Securing Remote Installation Services	234
Implementing Terminal Server Security	238
Securing Terminal Services	241
Implementing SNMP Security	244
Securing Community Memberships	245
Authorizing Management Stations	246
Securing SNMP Transmissions	247
Securing Servers Using Security Templates	247
Default Security Settings	248
Implementing Secure Access for NonMicrosoft Clients	250
Securing Network Access to UNIX Clients	251
Securing Network Access to Netware Clients	252
Securing Network Access to Macintosh Clients	253
Planning Best Practices	254
Chapter Summary	255
Key Terms	256
Review Questions	258
Hands-on Projects	261
Case Projects	263

CHAPTER SEVEN**Securing Network Communications 265**

Implementing Server Message Block Signing	266
Configuring SMB Security	266
Securing Network Traffic Using IP Security	271
Authentication Header Protocol	272
Encapsulating Security Payload	274
IPSec Modes	275
IPSec with Windows 2000	277
IPSec Policy Configuration	278
IPSec Policy Creation	283
IPSec Deployment	284
Planning Best Practices	287
Chapter Summary	288
Key Terms	288
Review Questions	289
Hands-on Projects	292
Case Projects	294

CHAPTER EIGHT**Securing Access For Remote Access Users 295**

Implementing and Configuring Routing and Remote Access	296
Configuring a Dial-up Server	296
Configuring Remote Access Clients	300
Implementing Virtual Private Network Access	302
VPN Server Configuration	305
VPN Client Configuration	307
Securing Remote Access	308
Configuring Remote Access Authentication	308
Configuring Callback Options	312
Remote Access Account Lockout	314
User Education	315
Remote Access Policies	316
Remote Access Policy Concepts	317
Configuring Remote Access Policies	318
Planning for Remote Access Policies	322
Internet Authentication Server	323
Introduction to Remote Authentication Dial-in User Service (RADIUS)	323
Implementing IAS as a RADIUS Server	326
Planning Best Practices	330
Chapter Summary	330
Key Terms	331
Review Questions	332
Hands-on Projects	336
Case Projects	339

CHAPTER NINE**Securing Access Between Corporate Locations 341**

Security Risks for Data Between Corporate Locations	342
Configuring Windows 2000 as a Router	345
Configuring Routing Options	345
Securing the Windows 2000 Router	357
Configuring and Securing Virtual Private Networks	360
VPN Tunneling Protocol Options	361
Configuring Secure Access to Partner Organizations	365
Securing Data Transmissions	365
Securing Resource Access to the Company Network	366
Planning Best Practices	368
Chapter Summary	368
Key Terms	369
Review Questions	370
Hands-on Projects	373
Case Projects	375

CHAPTER TEN**Designing Secure Access to the Internet 377**

Securing the Internal Network from the Internet	378
Network Address Translation	380
Configuring Firewalls	385
Implementing Demilitarized Zones	390

Securing User Access to the Internet	393
Implementing Proxy Services	394
Configuring Internet Clients	396
Planning Best Practices	402
Chapter Summary	403
Key Terms	404
Review Questions	405
Hands-on Projects	408
Case Projects	411
APPENDIX A	
Exam Objectives for MCSE Certification Exam #70-220: Designing Security for a Microsoft Windows 2000 Network	413
Analyzing Business Requirements	413
Analyzing Technical Requirements	414
Analyzing Security Requirements	415
Designing a Windows 2000 Security Solution	415
Designing a Security Solution for Access Between Networks	416
Designing Security for Communication Channels	417
GLOSSARY	419
INDEX	427

Preface

Welcome to the *MCSE Guide to Designing Microsoft Windows 2000 Security*! This book provides in-depth coverage of the knowledge and skills required to pass Microsoft certification exam 70-220: *Designing Security for a Microsoft Windows 2000 Network*. This course of study prepares a network professional to have the ability to design network security solutions. These solutions include analysing business requirements, identifying security needs, and applying the security recommendations to assist in the control and monitoring of network and service resources.

THE INTENDED AUDIENCE

The goal of this book is to teach strategies for security design to individuals who desire to learn about that topic for practical purposes, as well as those who wish to pass Microsoft exam, #70-220. This book provides the content for all the skills measured on that exam, but also provides related information that is not directly tested.

Chapter 1, “Identifying Security Risks” provides an overview of internal and external security risks and identifies general principals for managing those risks. Chapter 2 “Corporate Components to Security Planning” emphasizes the importance of collecting information before designing a security plan. It shows how to identify existing and planned business models, existing company processes, organizational structures, company strategies, and IT management structure. Chapter 3, “Securing Resources on Windows 2000 Servers” outlines how to control access to the various resources available on the network. Various authentication protocols are described and information is provided about how to plan and configure an audit policy.

Chapter 4, “Designing Active Directory for Security” identifies and explains various Active Directory components and how to design a secure Organizational Unit structure. This chapter teaches how to design and implement Account Policies, and how to delegate control of administrative tasks. It then describes how Group Policy can be used to configure and implement an effective security plan. Chapter 5, “Implementing a Public Key Infrastructure”, focuses on the concepts of Public Key Infrastructure and how it can be used to enhance security in Windows 2000.

Chapter 6 “Securing Network Services” describes how to implement Windows 2000 DNS and DHCP, and how to plan secure implementations of Remote Installation Services and SNMP, as well as secure access for non-Microsoft clients. The concept of securing servers

using Security templates is also discussed. Chapter 7 “Securing Network Communications” describes how to plan a secure network communication implementation using Server Block Signing. This chapter also teaches how to plan and implement secure network transmission by implementing IP security (IPSec).

Chapter 8 “Securing Access for Remote Access Users” looks at the issues involved in implementing access for dial-up clients and VPN clients. It also discusses enhanced security for Windows 2000 remote access, and how to plan and use remote access policies. RADIUS is also introduced to assist in situations where multiple RRAS servers are implemented.

Chapter 9 “Securing Access Between Corporate Locations” looks at the security risks that exist for information passing between corporate locations. This chapter also outlines how to implement and secure Windows 2000 when it is configured as a router, or as a VPN server. It then describes secure network access for partner organizations.

Chapter 10 “Designing Secure Access to the Internet” covers how to secure an internal corporate network by implementing various security services, such as NAT, firewalls, and Demilitarized Zones. It also describes secure user access through the use of proxy services, such as MS Proxy 2.0 and Internet Security and Acceleration Server 2000. In addition, this chapter teaches how to design and implement a corporate Internet usage policy.

FEATURES

To ensure a successful learning experience, this book includes the following pedagogical features:

- **Chapter Objectives:** Each chapter in this book begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with a quick reference to the contents of that chapter, as well as a useful study aid.
 - **Illustrations and Tables:** Numerous illustrations of server screens and components aid you in the visualization of common setup steps, theories, and concepts. In addition, many tables provide details and comparisons of both practical and theoretical information and can be used for a quick review of topics.
 - **End-of-Chapter Material:** The end of each chapter includes the following features to reinforce the material covered in the chapter:
 - **Summary.** A bulleted list is provided which gives a brief but complete summary of the chapter
 - **Review Questions.** A list of review questions tests your knowledge of the most important concepts covered in the chapter
 - **Key Terms List.** A list of all new terms and their definitions
-

- **Hands-on Projects.** Hands-on projects help you to apply the knowledge gained in the chapter
- **Case Study Projects.** Case study projects take you through real world scenarios
- **On the CD-ROM.** On the CD-ROM you will find **CoursePrep** exam preparation software, which provides 50 sample MCSE exam questions mirroring the look and feel of the MCSE exams

TEXT AND GRAPHIC CONVENTIONS

Wherever appropriate, additional information and exercises have been added to this book to help you better understand what is being discussed in the chapter. Icons throughout the text alert you to additional materials. The icons used in this textbook are as follows:



Tips are included from the author's experience and provide extra information on resources related to network design.



The Note icon is used to present additional helpful material related to the subject being described.



Each Hands-on Project in this book is preceded by the Hands-on icon and a description of the exercise that follows.



Case project icons mark the case project. These are more involved, scenario-based assignments. In this extensive case example, you are asked to implement independently what you have learned.

INSTRUCTOR'S MATERIALS

The following supplemental materials are available when this book is used in a classroom setting. All of the supplements available with this book are provided to the instructor on a single CD-ROM.

Electronic Instructor's Manual. The Instructor's Manual that accompanies this textbook includes:

- Additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.
 - Solutions to all end-of-chapter materials, including the Review Questions, Hands-on Projects and Case Projects.
-

ExamView. This textbook is accompanied by ExamView, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView includes hundreds of questions that correspond to the topics covered in this text, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers, and also save the instructor time by grading each exam automatically.

PowerPoint presentations. This book comes with Microsoft PowerPoint slides for each chapter. These are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel at liberty to add your own slides for additional topics you introduce to the class.

Read This Before You Begin

TO THE USER

This book was written with the network professional in mind. It provides an excellent preparation for the Microsoft exam 70-220, and also for the real-life tasks involved in designing network security for today's networks, which must support an ever-increasing variety of applications. To fully benefit from the content and the projects presented here, you will need access to a classroom lab containing computers configured as follows:

- Windows 2000 Advanced Server installed with the default settings. Name each computer server1, server2, etc. It is recommended to have 2 network cards in each computer.
- Run dcpromo.exe to upgrade the server to a domain controller. Install DNS when prompted. Use Lonestar.com as the domain name. Change the zone type to Standard Primary.
- For the Domain Users group, add the right to log on locally to the domain controllers security policy.

Visit Our World Wide Web Site

Additional materials designed especially for you might be available for your course on the World Wide Web. Go to *www.course.com*. Search for this book title periodically on the Course Technology Web site for more details.



TO THE INSTRUCTOR

The Hand-on projects should meet the hardware requirements listed below:

Hardware Component	Windows 2000 Advanced Server
CPU	Pentium II 200 or higher
Memory	128 MB RAM
Disk Space	1 GB minimum for partition containing system files
Drives	CD-ROM Floppy Disk
Networking	TCP/IP 2 Network adapters Card 1 – 131.107.1.1: Label: Internal Card 2 – 131.107.2.1: Label: External Install DHCP but do not activate the scope (scope: 131.107.1.5 – 131.107.1.10)
	A connection to the Internet via some sort of NAT or Proxy server is assumed.

1. Install Windows 2000 Advanced server. Name the computer **Server1**.
 2. Run dcpromo.exe to upgrade the server to a domain controller. Install DNS when prompted. Use Lonestar.com as the domain name. Change the zone type to Standard Primary.
 3. For the Domain Users group, add the right to log on locally to the domain controllers security policy.
 4. Detailed setup instructions for the labs are contained in the Instructor's Manual.
-